Phase-modulation transmission system for quantum cryptography

Jean-Marc Mérolla, Yuri Mazurenko, Jean-Pierre Goedgebuer, Henri Porte, and William T. Rhodes

GTL-CNRS Telecom, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz Laboratoire Optique P. M. Duffieux, UMR 6603, 25030 Besançon Cedex, France

Received August 25, 1998

We describe a new method for quantum key distribution that utilizes phase modulation of sidebands of modulation by use of integrated electro-optic modulators at the transmitting and receiving modules. The system is shown to produce constructive or destructive interference with unity visibility, which should allow quantum cryptography to be carried out with high flexibility by use of conventional devices. © 1999 Optical Society of America

OCIS codes: 060.2330, 060.5060, 350.2460, 270.0270.

Quantum key distribution, also termed quantum cryptography, allows a key to be shared by both the transmitter (Alice) and the receiver (Bob), even if the transmission channel is attacked, i.e., independently of the eavesdropper (whatever the technology to attack the channel is). In the quantum cryptographic devices used in optics,[1-3] one assumes that an eavesdropper, Eve, can attack the transmission line. The general procedure in quantum cryptography includes the following steps: First, Alice sends a sequence of photons, choosing randomly in which quantum state each of the photons is prepared. Each state serves to encode a bit of information. When receiving the photons, Bob tries to measure their state. Alice and Bob keep only the data from these correctly measured photons. As the line is trapped, the photon statistics are modified and the counting error rate is higher than that obtained, as there is no eavesdropper.

Ideally, the optical source used should be a quantum source emitting single photons.[4] Practically, pulsed lasers strongly attenuated such that they emit a number of photons per pulse much smaller than 1 (typically 0.1 photon/pulse) are used. Two main methods have been used to encode information. The first one is based on polarization-coded quantum states.[5] Each bit of information is coded in a photon with a given polarization state. The problem with this method is to preserve the photon polarization over a long transmission distance, especially in standard telecom fibers. Systems based on Faraday mirrors were proposed recently to overcome that drawback.[6] The second method is based on delay-coded quantum states.[7] In that case, each bit is encoded into an optical path difference in a way that is similar in many aspects to that used in coherence modulation of light,[8] except that the source is a quantum source and the detector is a photon counter. Practically, a pair of interferometers, with matched path imbalances greater than the pulse length, forms the transmitter and receiver. The difficulty in that case is to maintain the optical delay in the interferometers constant and free of mechanical vibrations and thermal drift.[7] Other solutions have also been proposed more recently that use schemes based on acousto-optic deflectors or multicolored photons[9] with, in the latter case, the theoretical demonstration of the possibility of using wavelengths to encode information.

In this Letter we report and evaluate a new encoding method whose peculiarity is to use a periodic phase modulation of light produced by integrated phase modulators in a way that is completely different from those of previous experiments. Alice encodes each bit of information into a frequency carrier with a phase that can be chosen randomly from two values. Similarly, Bob generates a frequency carrier with a phase that can be switched randomly between two states, in such a way that Bob can retrieve the states of the photons sent by Alice by using single-photon interference. In what follows, we report the principle of operation. Preliminary experimental results were carried out with a conventional source; they show that the method can be used for optical cryptography applications.

The system is shown schematically in Fig. 1. Alice's transmitter consists of a distributed-feedback Bragg laser diode and a phase modulator (PM$_1$). Another

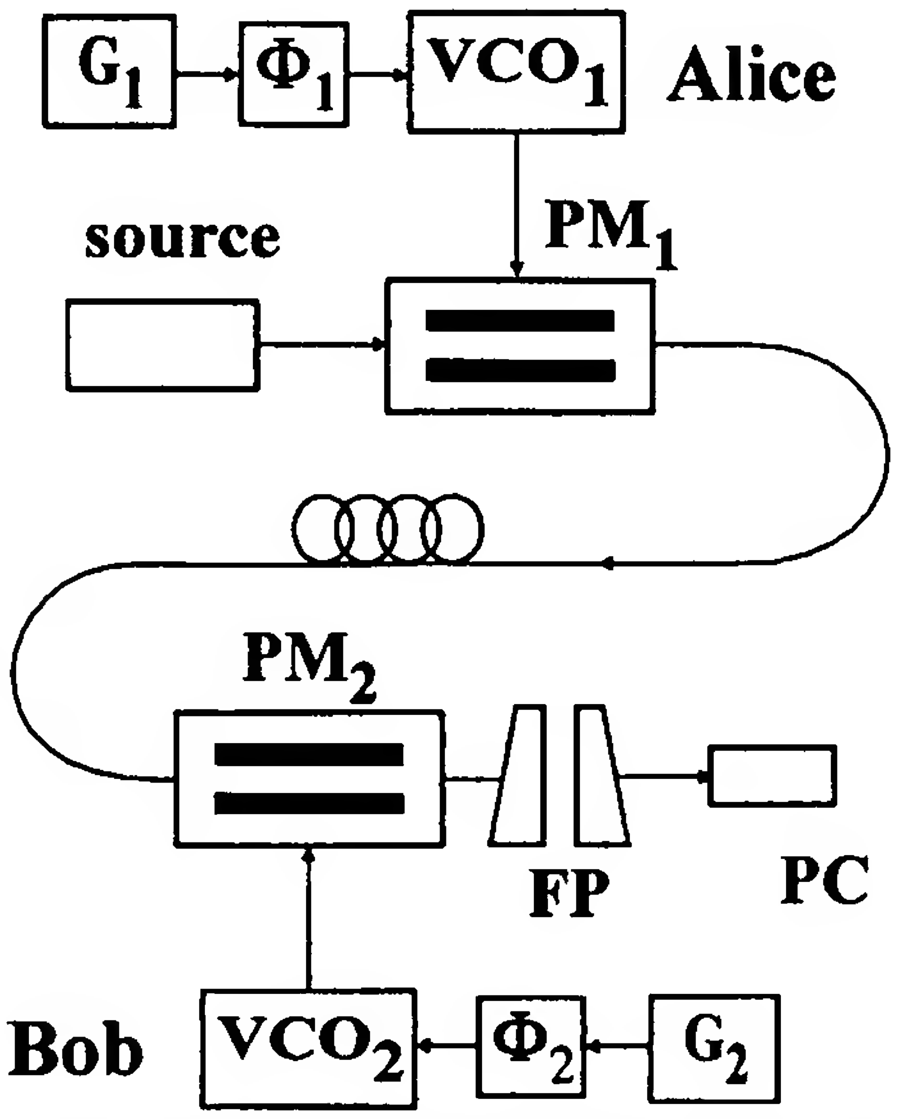


Fig. 1. Schematic diagram of the phase-modulation transmission system.

phase modulator (PM_2), a Fabry–Perot spectral filter (FP), and a photon counter (PC) form Bob's receiver. Voltage-controlled oscillators VCO_1 and VCO_2 drive Alice's and Bob's phase modulators, respectively. Alice's information bits are encoded by introduction of a phase shift Φ_1 in the modulation signal. Phase Φ_1 of VCO_1 can be switched by random-bit generator G_1 between 0 (bit 0) and $\pi/2$ (bit 1); phase Φ_2 of VCO_2 can be switched by random generator G_2 between π and $3\pi/2$. The light beam from the laser diode is referred to as the reference beam. This reference beam is phase modulated by PM_1, which is driven by a sine electrical signal at angular frequency Ω provided by oscillator VCO_1. Let E_0 and ω_0 be, respectively, the amplitude and the angular frequency of the input reference beam. At the first modulator output, the light field can be expressed as

$$E_1(t) = E_0 \exp j[\omega_0 t + m \cos(\Omega t + \Phi_1)], \qquad (1)$$

where $m = Ka/2$ is the modulation depth, a is the peak-to-peak amplitude of the electrical signal, $K = \pi/V_\pi$ is the modulation rate of the phase modulator, and V_π is its half-wave voltage. Assuming that the modulation depth is small ($m \ll 1$), Eq. (1) can be approximated as

$$E_1(t) = E_0 \exp(j\omega_0 t)[1 + jm \cos(\Omega t + \Phi_1)]. \qquad (2)$$

The power-spectrum density of $E_1(t)$ is formed by the original reference frequency ω_0 and two side frequencies $\omega_0 + \Omega$ and $\omega_0 - \Omega$. Those sidebands will be used as the information carriers for quantum transmission. Their intensity should be sufficiently weak that one can consider that there are single photons. The attenuation is achieved by control of modulation depth m and the intensity of the laser source to yield typically a number of photons per pulse much smaller than 1 for each of those sidebands.

Light field $E_1(t)$ is transmitted to modulator 2 (Bob) via a standard single-mode fiber that is the quantum transmission channel. Bob phase modulates its input optical signal with the same frequency Ω and modulation depth m as Alice, using VCO_2 that is synchronized with VCO_1. He introduces the phase Φ_B. Then the light field at Bob's modulator output can be written as

$$E_2(t) = E_0 \exp(j\omega_0 t)\{1 + 2jm \cos[(\Phi_1 - \Phi_2)/2] \times \cos[\Omega t + (\Phi_1 + \Phi_2)/2]\}. \qquad (3)$$

The power-spectrum density of $E_2(t)$ is formed by a central peak of frequency ω_0 and two side peaks at $\omega_0 + \Omega$ and $\omega_0 - \Omega$, whose intensity is given by

$$i = (m^2|E_0|^2)/2 \cos^2[(\Phi_1 - \Phi_2)/2]. \qquad (4)$$

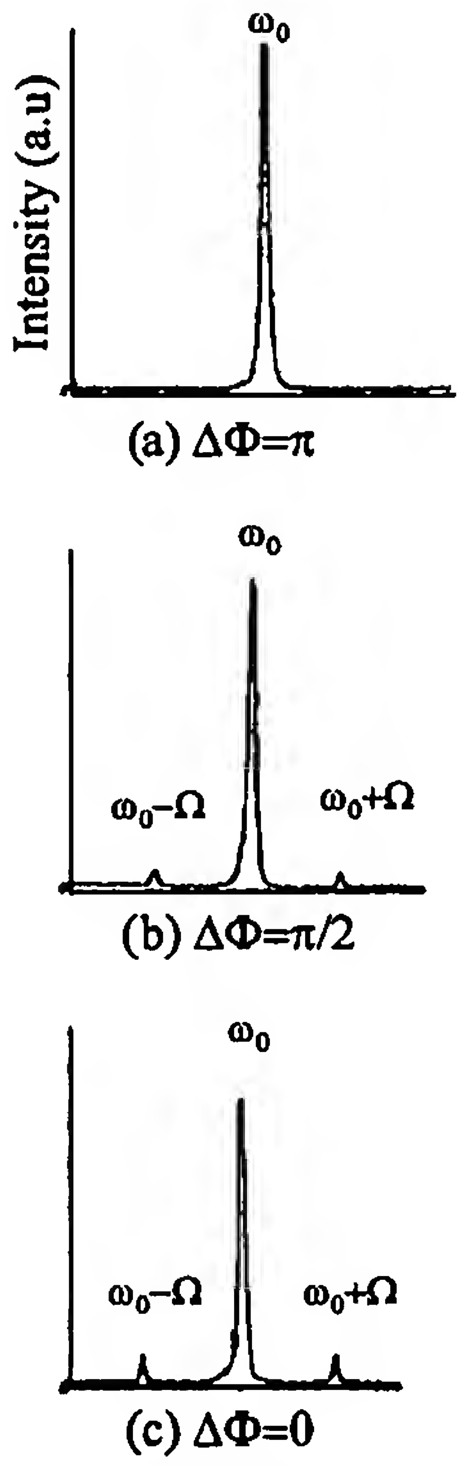
Then the intensity in the center peak is approximately $I = |E_0|^2/2 - 2i \approx |E_0|^2/2$.

It can be clearly seen that the intensity in the sidebands depends on the values of the phases Φ_1 and Φ_2 chosen by Alice and Bob. As $|\Phi_1 - \Phi_2| = 0$, i is maximum (constructive interference between Alice's and Bob's side modes), and it is minimum as $|\Phi_1 - \Phi_2| = \pi$ (destructive interference), whereas the intensity in the center peak can be considered constant because the modulation depth is small.

Detecting the intensity i in the sidelobes is carried out with a Fabry–Perot interferometer whose transmission peak is adjusted on one of the sidebands $\omega_0 \pm \Omega$ and by a photon detector. It can be clearly seen that, when the system operates with single photons in a sideband, Eq. (4) yields single-photon interference at the Fabry–Perot output. This forms the principle of operation for exchanging a secret key between Alice and Bob. In fact, Eq. (4) corresponds to the ideal situation of a Fabry–Perot interferometer with infinite finesse, i.e., with a high spectral resolution and a monochromatic light source. Practically, intensity i detected in a side peak also contains a spurious term that is related to the interferometer's finesse F and to the central lobe, which is not completely filtered out.

The experimental demonstration was implemented with a cw distributed-feedback Bragg laser diode operating at 1 dBm at a 1558-nm wavelength. Its linewidth was 1 MHz. The modulators used were electro-optic phase modulators integrated in $LiNbO_3$, with half-wave voltage $V_\pi = 5$ V. Their electrical bandwidth and optical transmission loss were 500 MHz and 4 dB, respectively. They were driven by two synchronized VCO's operating at 300 MHz. Their phases could be changed independently and tuned on Φ_1 and Φ_2 by a phase shift driver with a bandwidth of 10 kHz. The driving voltages applied to the modulators were 300-MHz sine signals with a peak-to-peak voltage $a = 1$ V. The modulation depth as defined above obtained was $m = 0.3$ rad. The Fabry–Perot interferometer at the system output was a scanning interferometer operating as an optical spectrum analyzer. It featured a finesse of 55, a free spectral range of 1 GHz, and a spectral bandwidth of 18 MHz. Its scanning range was 800 MHz. Then the two sidebands and the reference center frequency could be observed simultaneously at its output. The power loss of the transmission system including the two modulators (4-dB loss/modulator), the fiber (20 km long, 0.18-dB/km loss), and the optical spectrum analyzer (3 dB loss) was ~15 dB. The bandwidth of the detector was 30 MHz. Under these conditions, though the system did not operate in the quantum regime, the validity of the principle of operation was checked easily.

Figure 2 shows the power-spectrum density thus obtained at the spectrum analyzer output for three values of $|\Phi_1 - \Phi_2|$. Each side mode is separated from the reference frequency by 300 MHz. In Fig. 2(a), Alice and Bob are out of phase, and the reference peak at ω_0 only is obtained (destructive interference). In Fig. 2(b), the phases are in quadrature. The sidebands at $\omega_0 \pm \Omega$ can be clearly seen; the center reference peak is slightly decreased. In Fig. 2(c), Alice and Bob are in phase. The sidebands reach a maximum (constructive interference) and the center peak decreases to a minimum (20% below its peak value),



(a) $\Delta\Phi=\pi$

(b) $\Delta\Phi=\pi/2$

(c) $\Delta\Phi=0$

Fig. 2. Experimental power spectra obtained with a scanning Fabry–Perot interferometer for phase shifts $\Delta\Phi$.

as predicted above. Such a detectable intensity variation in the center peak could be used directly by an eavesdropper. However, for the system to operate as a quantum key distribution system the number of photons in the sideband frequencies should be typically of the order of 0.1, yielding ten times more photons in the center peak for the modulation depth $m = 0.3$ chosen. The variance of the photon number in the center peak is then 1, a value that is large compared with the intensity variation of 20% mentioned above. Such an intensity variation is then masked by the photon noise and will not be detected by an eavesdropper. Another point to consider is the visibility of the interference that occurs at a sideband as the phase difference $|\Phi_1 - \Phi_2|$ is varied. It was measured to be 93%, to be compared with a theoretical visibility of 98% as the interferometer's finesse is 55. The difference is probably due to slight defects in the alignment of the mirrors of the optical spectrum analyzer. It seems possible to increase the visibility to 99% by use of a fiber Fabry–Perot interferometer with a finesse of 100. Let us also note finally that the achieved system can easily be made polarization independent by use of $LiNbO_3$ integrated x-cut, z-propagating Mach–Zehnder modulators such as those described in Ref. 10.

In summary, we have reported a new transmission system that uses interference between phase-modulated sidebands in the spectral domain. The method has been demonstrated experimentally by use of a classical source that yields high interference visibility. Recent experiments confirm that the system, which is very simple, can operate in the quantum regime by using the same source intensity modulated to produce 50-ns-duration pulses at repetition rate of 1 MHz and attenuated such that the average number of photons in a sideband is 0.1. The visibility thus obtained in the quantum regime is 91%.

J.-M. Mérolla's research was funded by the Délégation Générale à l'Armement. We thank France Telecom for its financial support. J.-M. Mérolla's e-mail address is xavier.rejeaunier@univ-fcomte.fr.

References

1. C. H. Bennet, Phys. Rev. Lett. **68,** 3121 (1992).
2. A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69,** 1293 (1992).
3. S. J. D. Phoenix and P. D. Townsend, Br. Telecom Technol. J. **11,** 66 (1993).
4. A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47,** 460 (1981).
5. J. Breguet, A. Muller, and N. Gisin, J. Mod. Opt. **41,** 2405 (1994).
6. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70,** 793 (1997).
7. P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron Lett. **29,** 634, 1291 (1993); C. Marand and P. D. Townsend, Opt. Lett. **20,** 1695 (1995).
8. J. P. Goedgebuer, J. Salcedo, and J. C. Vienot, Opt. Acta **29,** 471 (1982); J. L. Brooks, R. M. Wentworth, R. C. Youngquist, M. Tur, B. Y. Kim, and M. J. Shaw, IEEE J. Lightwave Technol. **3,** 1062 (1985).
9. P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20,** 1062 (1995); D. N. Klyshko, Phys. Lett. A **227,** 1 (1997).
10. C. C. Chen, H. Porte, A. Carenco, and J. P. Goedgebuer, IEEE Photon. Technol. Lett. **9,** 1363 (1997).